REMARKS

Applicants respectfully traverse the rejections of the pending claims.

Authentication methods in digital rights management (DRM) schemes are known. Indeed, both the Graunke reference (USP 5,991,399) and the Richard reference (USP 5,992,074) recognize their use. Content providers provide digital certificates to content users so that they become authorized to access protected content. For example, a user at a host device such as a personal computer may obtain a digital certificate that is then provided to a storage engine controlling access to protected content stored on a storage medium. The authentication process comprises verifying a digital signature provided by the content provider that is contained within the digital certificate. Once the signature is authorized, the user is authenticated and may proceed to access the protected content.

However, because digital signatures involve the use, typically, of private/public key cryptography that may become compromised, there is another layer of protection commonly available in conventional DRM schemes. That layer would be the revocation process, which follows authentication. In other words, even though a user may possess a valid certificate, if that user is identified by a revocation list, the user is denied access to the protected content. As is conventional, this revocation scheme follows authentication. It is performed as an initial handshaking routine between the host device and the storage engine.

In contrast to the conventional revocation scheme just discussed, the present invention provides a file-by-file revocation scheme. It is not performed immediately following authentication but instead is much more granular in that it precedes any file request by the host device. Consider, for example, pages 32 and 33 of the disclosure. As

set forth by the Applicants, in their revocation scheme, each file may have its own associated revocation list, see for example, lines 21 through 23 on page 32. As such, this type of revocation would not be performed immediately after authentication – a user may or may not desire access to any given file on the storage medium. Not only do the Applicants provide greater granularity and control, the revocation itself is more adaptable in that the associated revocation list with a given file comprises a set of rules for evaluating fields in the digital certificate against data in the revocation list, see for example lines 24 through 28 on page 32.

These advantageous features of Applicants revocation scheme are reflected in the claims. For example, claim 36 recites a revocation method including the acts of: authenticating the digital signature; receiving at the storage engine a file request from the host device, the file request being directed to a file stored on a storage medium accessible to the storage engine; reading a revocation file associated with the file from the storage medium, the revocation file containing at least one rule, the at least one rule associating data in the revocation file with data in certificate; applying the at least one rule on the data in the revocation file and the associated data in the certificate; and if the application of the at least one rule provides a failing result, denying the file request.

In sharp contrast, Nonaka reference (US 2003/0046238) plainly discloses a conventional (and non-granular) revocation scheme. As shown on the cover page, Nonaka discloses a content distribution scheme to a series of networked "audio-visual machines" (elements 160). Each A/V machine includes a "secure application module (SAM)" (elements 105). In this network, a SAM 105_1 obtains a registration list of all the networked SAMs and creates a SAM registration list (paragraphs 667, 668, Fig. 59).

SAM_1 provides this registration list to the "EMD service center" (element 102), which checks its revocation list to see if any rogue SAMs are in the list (paragraph 671).

As seen in Figure 30 and discussed in paragraph 251, SAM 105_1 includes a flash memory storage unit 192. This storage unit stores (among other things) a revocation list of devices (paragraph 435). In paragraphs 671 through 675, Nonaka explains how the SAMs update each other's revocation list as well as receiving updates from the EMD service center.

That is all Nonaka has to say about revocation – Nonaka's revocation is plainly not granular, indeed, Nonaka makes no mention whatsoever regarding individual file system objects within the content being distributed from content provider 101 in Figure 1. Instead, there is just "content." When a SAM gets content, he is checked for revocation just as in any conventional DRM scheme. There is absolutely no suggestion or teaching within Nonaka for the claimed acts of revoking on a file-by-file basis such that a given device might be revoked for one file yet have permission to access another. Instead, the Nonaka revocation scheme is non-granular: either a Nonaka device is revoked or it is not. If a Nonaka device is revoked, then it has no ability to access any content. Accordingly, the pending claims are patentable over Nonaka.

CONCLUSION

For the above reasons, pending Claims 36-40, 42, and 43 are in condition for allowance and allowance of the application is hereby solicited. If the Examiner has any

questions or concerns, a telephone call to the undersigned at (949) 752-7040 is welcomed and encouraged.

Certification of Facsimile Transmission
I hereby certify that this paper is being facsimile transmitted to the U.S. Patent and Trademark Office on the date shown below.

Saundra Carr — October 21, 2005
Saundra Carr — Date of Signature

Respectfully submitted,

Jonathan W. Hallman
Attorney for Applicants
Reg. No. 42,622